APTRS: Privilege Escalation via Mass Assignment of is_superuser in User Edit Endpoint

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-34406
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-31 22:16:18 UTC
Updated	2026-04-01 14:23:37 UTC
Description	APTRS (Automated Penetration Testing Reporting System) is a Python and Django-based automated reporting tool design

Risk And Classification

Primary CVSS: v4.0 9.4 CRITICAL from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000960000 probability, percentile 0.265940000 (date 2026-04-01)

Problem Types: CWE-915 | CWE-915 CWE-915: Improperly Controlled Modification of Dynamically-Determined Object Attributes

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	9.4	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/
4.0	CNA	DECLARED	9.4	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	APTRS	APTRS	affected < 2.0.1	Not specified

References

Reference	Source	Link	Tag
github.com/APTRS/APTRS/releases/tag/2.0.1	security-advisories@github.com	github.com	
github.com/APTRS/APTRS/security/advisories/GHSA-gv25-wp4h-9c35	security-advisories@github.com	github.com	
github.com/APTRS/APTRS/commit/d1f1b3a5d1953082af8e075712ca29742e900d56	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.